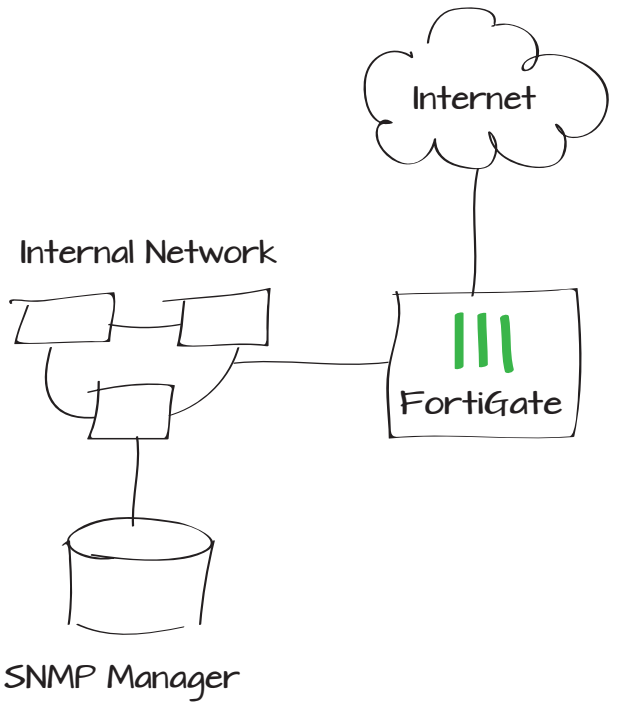
Using SNMP to monitor the FortiGate unit

The Simple Network Management Protocol (SNMP) enables you to monitor hardware on your network. You configure the hardware, such as the FortiGate SNMP agent, to report system information and send traps (alarms or event messages) to SNMP managers.

In this example, you configure the FortiGate SNMP agent and an example SNMP manager so that the SNMP manager can get status information from the FortiGate unit and so that the FortiGate unit can send traps to the SNMP manager.

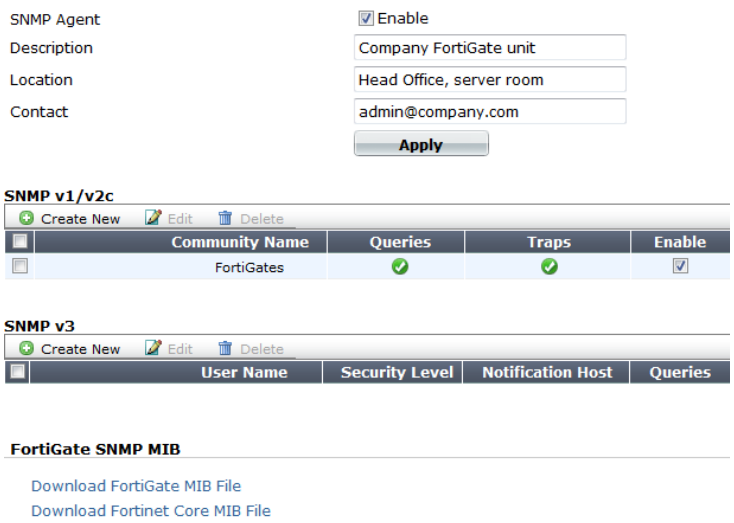
1. Configuring the FortiGate SNMP agent
2. Enabling SNMP on a FortiGate interface
3. Downloading Fortinet MIB files to and configuring an example SNMP manager
4. Results



Configuring the FortiGate SNMP agent

Go to **System > Config > SNMP**.

Configure the SNMP agent.

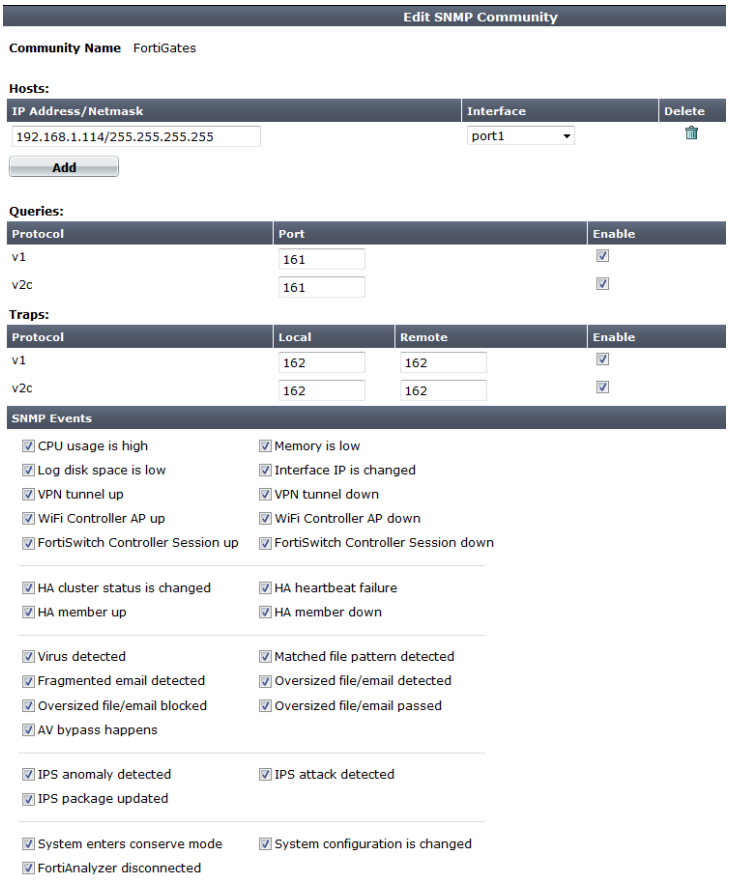


Under **SNMP v1/v2c** create a new community.

Add the IP address of SNMP manager (in the example, 192.168.1.114/32). If required, change the query and trap ports to match the SNMP manager.

You can add multiple SNMP managers or set the IP address/Netmask to 0.0.0.0/0.0.0.0 and the Interface to ANY so that any SNMP manager on any network connected to the FortiGate unit can use this SNMP community and receive traps from the FortiGate unit.

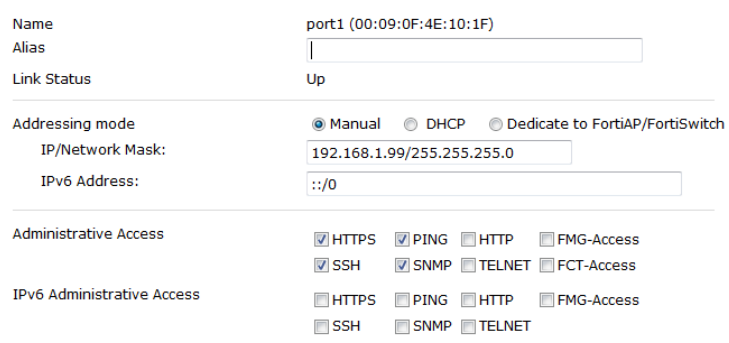
Enable the **SNMP Events** (traps) that you need. In most cases leave them all enabled.



Enabling SNMP on a FortiGate interface

Go to **System > Network > Interfaces**.

Enable SNMP administrative access on the interface connected to the same network as the SNMP manager.

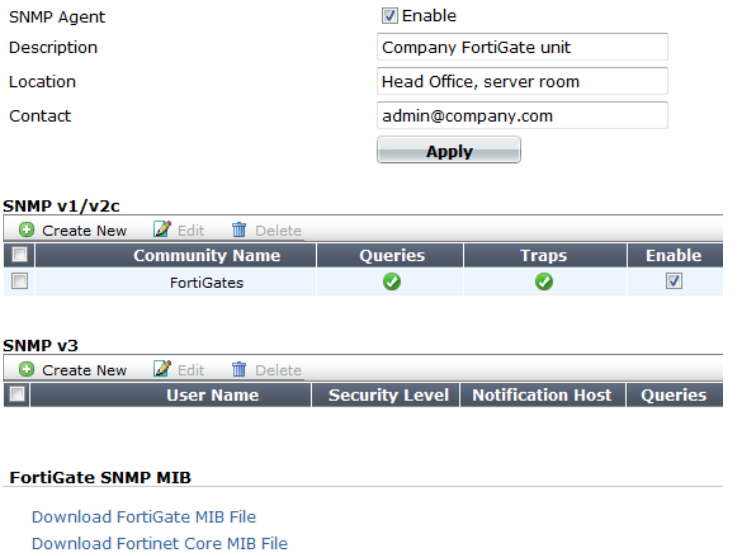


Downloading the Fortinet MIB files to and configuring an example SNMP manager

Go to **System > Config > SNMP** to download FortiGate SNMP MIB file and the Fortinet Core MIB file.

Two types of MIB files are available for FortiGate units: the Fortinet MIB, and the FortiGate MIB. The Fortinet MIB contains traps, fields, and information that is common to all Fortinet products. The FortiGate MIB contains traps, fields, and information that is specific to FortiGate units.

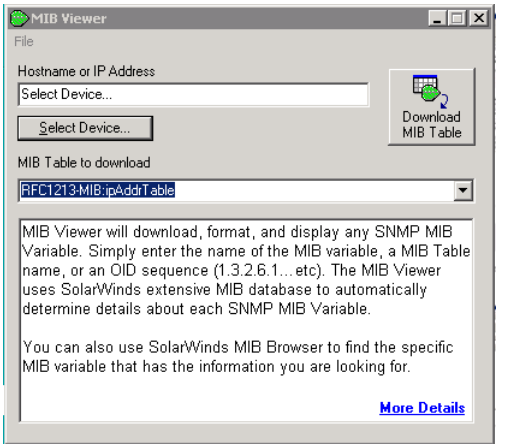
Configure the SNMP manager at 192.168.1.114 to receive traps from the FortiGate unit. Install the FortiGate and Fortinet MIBs.



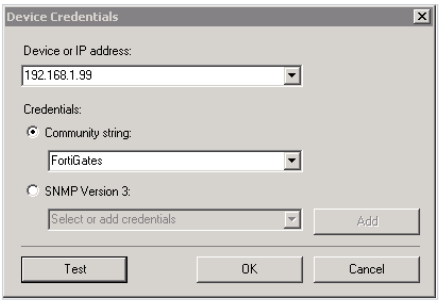
Results

This example uses the SolarWinds SNMP trap viewer.

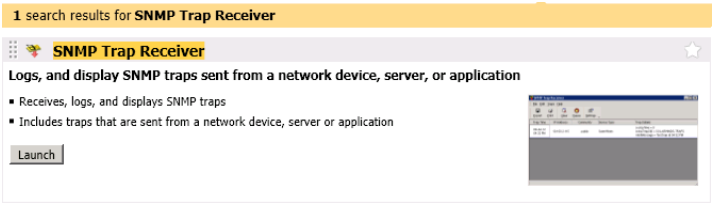
In the SolarWinds Toolset Launch Pad, go to **SNMP > MIB Viewer** and select **Launch**.

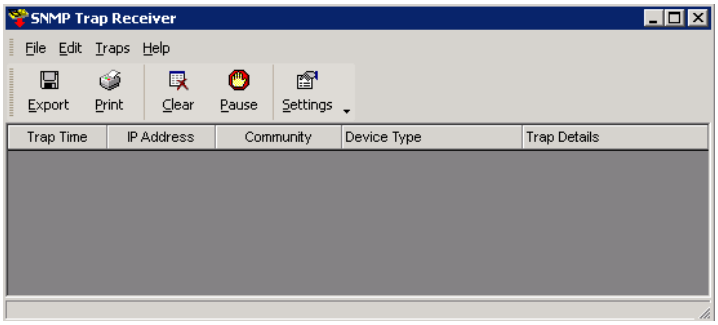


Choose **Select Device**, enter the IP address of the FortiGate unit, and choose the appropriate community string credentials.



Open the SNMP Trap Receiver and select **Launch**.





On the FortiGate unit, perform an action to trigger a trap (for example, change the IP address of the DMZ interface).

Verify that the SNMP manager receives the trap.

Trap Time	IP Address	Community	Device Type	Trap Details
08-Mar-13 10:49 AM	192.168.1.99	FortiGates		sysUpTime = 6976332 snmpTrapOID = fnTrapInfChg.1.3.0.201 fnTrapInfChg.1.1.1 = FG100D3G12801361 sysName = FG100D3G12801361 ifIndex = 2
08-Mar-13 10:49 AM	192.168.1.99	FortiGates	fnTrapSystem.1.1004	sysUpTime = 6976332 snmpTrapOID = fnTrapSystem.1.1004.0.201 fnTrapInfChg.1.1.1 = FG100D3G12801361 sysName = FG100D3G12801361 ifIndex = 2 experimental.1057.1 = 192.168.1.99
08-Mar-13 10:49 AM	192.168.1.99	FortiGates		sysUpTime = 6976332 snmpTrapOID = fnTrapSystem.6.0.1004 fnTrapInfChg.1.1.1 = FG100D3G12801361 ifName.2 = dmz fnTrapSystem.6.2.1 = 10.10.10.1 fnTrapSystem.6.2.2 = 255.255.255.0
08-Mar-13 10:49 AM	192.168.1.99	FortiGates	fnTrapSystem.1.1004	sysUpTime = 6976332 snmpTrapOID = fnTrapSystem.1.1004.0.1004 fnTrapInfChg.1.1.1 = FG100D3G12801361 ifName.2 = dmz fnTrapSystem.6.2.1 = 10.10.10.1 fnTrapSystem.6.2.2 = 255.255.255.0 experimental.1057.1 = 192.168.1.99

On the FortiGate unit, view log messages showing the trap was sent by going to **Log & Report > Event Log > System**.

cfgpath	system.interface	**Date/Time**	10:49:28 (Fri Mar 8 10:49:28 2013)
Virtual Domain	root	**Level**	information
Timestamp	Fri Mar 8 10:49:28 2013	**cfgtid**	2949201
logid	44547	**Sub Type**	system
User Interface	GUI(172.20.120.21)	**User**	admin
Action	Edit	**cfgobj**	dmz
roll	65409	**cfgattr**	ip[10.10.10.99 255.255.255.0->10.10.10.1
Message	Edit system.interface dmz		